

RTP:RCH/EMR
F.#2017R01784

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH THE
EMAIL ADDRESS
"MCGOLFO@GMAIL.COM" THAT IS
STORED AT PREMISES CONTROLLED
BY GOOGLE, INC.

TO BE FILED UNDER SEAL

**APPLICATION FOR A
SEARCH WARRANT FOR
INFORMATION IN
POSSESSION OF A PROVIDER
(EMAIL ACCOUNT)**

Case No. 19-278M

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, MELISSA GALICIA, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain email account, specifically "Mcgolfo@gmail.com" (the "SUBJECT EMAIL ACCOUNT"), that is stored at premises controlled by Google, Inc. ("Google"), an email service provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation, and have been for more than three years. I have participated in numerous investigations involving search warrants, including the execution of search warrants on places of business, private homes, and arrest warrants. As a result of my training and experience, I am familiar with the techniques and methods of operation used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 666 (theft concerning programs receiving federal funds) and 18 U.S.C. § 1347(a) (health care fraud) have been committed by Marina Golfo. There is also probable cause to search the information described in Attachment A for evidence of these crimes as further described in Attachment B.

I. PROBABLE CAUSE

A. BACKGROUND

5. In April 2017, the New York City Department of Investigation (“DOI”) initiated an investigation into fraudulent billing allegations in connection with the New York State Early Intervention Program (“EIP”). EIP is a New York State program that provides remedial services to developmentally delayed children from birth to age three. Such services may include physical, occupational, and speech therapy; special instruction; and social work services. These services are provided by individual therapists who are either subcontractors or employees of agencies that hold

contracts with the New York State Department of Health (the “NYSDOH”). The New York City Department of Health and Mental Hygiene (the “DOHMH”) administers EIP in New York City and conducts audit, quality assurance, and compliance oversight of EIP. While the majority of costs associated with EIP treatment are covered by New York State funding, some of the cost is covered by city and federal funding, as well as, occasionally, private insurers.

6. The DOI investigation concerned allegations that certain therapists employed by agencies holding EIP contracts who were assigned to treat developmentally delayed children were instead, at various points, forging session notes and invoices for treatment sessions that never occurred. As a result, these individuals were receiving payment for non-existent treatment sessions. In order to receive payment for an EIP therapy session, a therapist must provide a written report documenting his/her session with a child. Sessions generally occur in half-hour or one-hour increments. These session notes detail the date, time and place of the session as well as some details of the therapy given and the child’s progress in response to the treatment. Session notes must be signed by the therapist and the parent or guardian of the child immediately after the EIP therapy session ends.

7. The DOI investigation revealed that Marina Golfo (“Golfo”), acting as an EIP therapist, forged numerous session notes, billed for those non-existent therapy sessions and received payment for these EIP services that she never provided. DOI investigators reviewed EIP session notes and invoice data that Golfo submitted between approximately January 2016 and September 2018. From their review of these records, DOI investigators uncovered numerous examples of potentially forged session notes for sessions that never occurred.

8. As part of the investigation, DOI investigators interviewed the parents of children identified in numerous session notes as the patients of Golfo. Several parents and guardians who

reviewed the relevant session notes confirmed to DOI investigators that Golfo had not in fact provided therapy sessions to the children identified in the session notes. Further, the notes documenting these alleged sessions were forgeries, oftentimes containing the forged signature of the parent or an unauthorized photocopy of the parent's signature. In addition, DOI investigators also spoke with parents who informed the investigators that no session occurred at dates and times for which Golfo had claimed a session was performed in her session notes.

9. Specifically, law enforcement officers determined that, between approximately April 2015 and September 2018, Golfo submitted fraudulent session notes and invoices and received payment for more than 1,500 non-existent EIP sessions, resulting in the improper disbursement of more than \$10,000 in Medicaid funds and more than \$146,000 in NYC DOHMH funds. For example:

a. Law enforcement officers interviewed the parents or guardians of children to whom Golfo claimed to provide EIP therapy sessions. Law enforcement officers identified numerous occasions in which Golfo claimed to perform an EIP therapy session, but which the parent or guardian stated did not occur as billed, including numerous occasions when the parent or guardian stated that their signature on the session note submitted by Golfo for the EIP therapy session was, in fact, a forgery.

b. Law enforcement officers also reviewed session notes submitted by Golfo, and observed that numerous session notes or parts of session notes including signatures, were photocopied.

c. Law enforcement officers reviewed telephone toll records for GOLFO's cellular telephone, which they identified as Golfo's cellular telephone based on, among other things, EIP employment records, and determined that on numerous occasions Golfo used her cellular telephone during at least a quarter of the time period that she claimed to be performing an EIP therapy session.

d. Law enforcement officers obtained historical location data for Golfo's cellular telephone. Law enforcement officers compared the historical location data to location information contained in the EIP session notes submitted by Golfo and determined that, on numerous occasions, Golfo was not present in the vicinity of the EIP therapy session location at the time of the purported EIP therapy session.

e. Law enforcement officers also reviewed toll records for Golfo's cellular telephone and found that, on many occasions, those records identified the geographic region where GOLFO was located at the time of a telephone contact. On numerous occasions, Golfo submitted a fraudulent EIP invoice for a purported EIP therapy session when the toll records reflected that Golfo was not in the geographic region of the EIP therapy session at the time she claimed the session took place.

f. Law enforcement officers also obtained license plate recognition ("LPR") records for a vehicle registered to Golfo. Law

enforcement officers compared LPR records to the EIP invoices submitted by Golfo and determined that, on numerous occasions, Golfo submitted an invoice for an EIP therapy session when LPR records reflected that her vehicle was not in the vicinity of the EIP therapy session location at the time of the purported session.

g. Law enforcement officers also reviewed travel records associated with Golfo, and determined that, on numerous occasions, Golfo submitted an invoice for an EIP therapy session when her travel records reflected that she was outside of New York at the time of the purported session.

10. On or about October 4, 2018, Golfo was arrested pursuant to an arrest warrant issued by the Honorable Vera M. Scanlon, United States Magistrate Judge for the Eastern District of New York. Incident to her arrest, law enforcement officers seized a cell phone belonging to Golfo (the "Cell Phone").

B. THE SUBJECT EMAIL ACCOUNT

11. On or about October 19, 2018, the Honorable Cheryl L. Pollack, United States Magistrate Judge for the Eastern District of New York, issued a search warrant authorizing the search of the Cell Phone recovered incident to Golfo's arrest.

12. Pursuant to the search warrant, law enforcement officers searched the Cell Phone and recovered emails received and sent by the SUBJECT EMAIL ACCOUNT, including numerous emails discussing the session notes and billing records submitted to EIP agencies, as well as numerous emails containing travel records which reflected that Golfo was outside of New York at the time of sessions she claimed to have completed.

13. For example, numerous emails sent by Golfo within the SUBJECT EMAIL ACCOUNT contained session notes as an attachment, which she sent to the EIP agencies that she worked with. Although the attachments are visible on the Cell Phone, they cannot be opened or accessed from the Cell Phone.

14. Numerous emails sent and received by Golfo within the SUBJECT EMAIL ACCOUNT concerned incidents where Golfo submitted overlapping session notes, session notes that were photocopied, session notes that were missing required information, or incidents where Golfo did not submit session notes that she billed for. For example:

- a. In June 2018, Golfo received multiple emails from an email address associated with Our Children First, one of the EIP agencies that she worked with, asking that she resubmit her session notes because the dates and signatures were cut off or because the notes were missing.
- b. In March 2018, Golfo became aware of an overlap in billing that needed to be fixed. On March 16, 2018, at approximately 10:24 am, Golfo wrote in substance and in part, "I definitely saw this kid at my normal time but I don't want to argue with these people I don't even see him anymore and hardly remember that day it was so long ago."
- c. On September 8, 2017, Golfo received an email from All About Kids, which was another one of the EIP agencies that she worked with, that stated in substance and in part, "Unfortunately, there is overwhelming evidence from your own session note documents that the signatures on the notes in question were part of whole pages that had been duplicated. Ever spacing, stroke, mark and letters on one page, including signatures, is a perfect match and alignment with other pages."

- d. Between October 2015 and July 2016, Golfo sent herself multiple emails from the SUBJECT EMAIL ACCOUNT in which the subject line appeared to refer to EIP sessions she completed and the times of the sessions. For example, on October 8, 2015, Golfo emailed herself a message with the subject line, "8:35-11:35 emma (3)." In my training and experience, this subject line referred to sessions she completed with a child named Emma for three hours. Law enforcement officers reviewed Golfo's session notes for October 8, 2015, and observed that she submitted session notes claiming that she provided four hours of sessions that day.

15. Numerous emails within the SUBJECT EMAIL ACCOUNT emails contained travel records which reflect that Golfo was outside of New York at the time of sessions she claimed to have completed. For example:

- a. On March 30, 2018, Golfo received an email from Delta Air Lines regarding her reservation for a flight from New York City to Burlington, Vermont, which was scheduled to depart New York on Thursday, August 23, 2018 at 11:25 a.m. and return to New York on Friday, August 24, 2018 at 6:18 p.m. Law enforcement officers reviewed Golfo's session notes for August 23 and August 24, 2018, and observed that she submitted session notes claiming that she provided four hours of sessions in New York each day, between 4:00 p.m. and 8:00 p.m.
- b. On June 26, 2017, Golfo received an email from Delta Air Lines regarding her reservation for a flight from New York City to Charlotte, North Carolina, which was scheduled to depart New York on Thursday, August 24, 2017, at 4:59 pm, with a return flight on Saturday, August 26, 2017. Law enforcement officers reviewed

Golfo's session notes for Friday, August 25, 2017, and observed that she submitted session notes claiming that she provided four hours of sessions that day.

16. On or about February 22, 2019, a grand jury sitting in the Eastern District of New York returned a two-count indictment against Marina Golfo, charging her with: (i) theft concerning programs receiving federal funds, in violation of 18 U.S.C. § 666(a)(1)(A); and (ii) health care fraud, in violation of 18 U.S.C. § 1347(a), between April 2015 and September 2018.

II. BACKGROUND ON GOOGLE ACCOUNTS

17. Google is a United States company that provides a variety of services that can be accessed from traditional computers and other electronic devices running various operating systems via web browsers or mobile and desktop applications created by Google ("apps"). As described in further detail below, the services include email, file storage and management, voice over internet calling, electronic messaging, and Internet search.

18. *Gmail*. In my training and experience, I know that Google allow subscribers to obtain email accounts at the domains gmail.com and googlemail.com. Subscribers obtain an account by registering with Google, and store, send, and receive email by accessing Google's servers. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users and the communications themselves may discuss crimes or reflect a conspiracy to do so. Similarly, users can send and receive emails with attached documents and other types of files, such as audio

recordings, video files, and photographs, to their emails which may themselves constitute evidence of the crimes under investigation.

19. *Google Calendar and Contacts.* Google account holders can also maintain address books, contact or buddy lists and calendar data on servers maintained and/or owned by Google. In my training and experience, evidence of who was using a Google account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files. Calendar and contact information can also assist investigators to identify coconspirators, and provide contextual information necessary to understand other evidence obtained in the investigation, for example, the significance of a presentation slide deck shown at a meeting documented in a calendar event, and a subsequent email confirming an understanding reached at the meeting.

20. *Google Hangouts.* Google Hangouts is a unified communications service that allows Google account holders to initiate and participate in text, voice or video chats, either one-on-one or in a group. Hangouts is a communication service built into Google+ and Gmail. Google Hangouts can also integrate with Google Voice, allowing users of that service to make free domestic phone calls from their electronic devices. Google offers Hangouts mobile apps for download that can be used on electronic devices running Apple's iOS or Google's Android operating systems.

21. *Google Plus.* Google also operates a free-access social networking website called Google+, located at www.plus.google.com. Google+ allows Google account holders to share written news, photographs, videos, and other information with other Google+ users who following the user, or with "collections" or "communities" followed by Google+ users. Google+ users can also post comments in response and choose to share them with other users.

22. *Google Voice.* In my training and experience, Google also provides its users with the ability to make and receive audio calls and to send and receive text messages over the Internet directly to traditional telephones. Google calls its service “Google Voice” and allows its users to obtain a free telephone number associated with their Google Voice account that will allow them to receive calls, text messages, and voicemail messages through Google Voice. Indeed, Google Voice is capable of transcribing a user’s voicemail messages and rendering them text searchable. Audio and video calls can be made using Google Voice from a user’s computer or smartphone as long as the user is connected to the Internet. Thus, Google retains records of such calls, but a user’s telephone service provider does not retain call history reflecting Google Voice calls. To offer these services, Google Voice saves and processes its users’ call, text, and voicemail information.

23. *Web & App Activity.* Google collects and retains a wide variety of data on its account holders’ use of Google applications and services. The data collected and retained by Google includes the following:

a. *Location History.* Google collects data on the location of their users from their electronic devices. Google uses this information for, among other things, location-based advertising, location-based search results, embedding location information in the photographs and videos taken by the user (known as geo-tagging), navigation through the “Google Maps” service and related applications, and features that permit users to locate their mobile electronic devices if they lose them.

b. *Browser and Search History.* Google operates a popular Internet search engine, browser software that runs on both traditional computers and on mobile electronic devices, and an operating system for mobile electronic devices. Google retains browser and

search history when a user views a web page or conducts an Internet search while logged into their Google account, or when they use Google's "Chrome" web browser or another Google desktop or mobile app to browse or search the Internet. Google account holders can also choose to synchronize Chrome data, including bookmarks, browser and search history, passwords, and other settings across multiple electronic devices when the user is signed into Chrome on each device. By default, when a user signs in to Chrome, all the user's Chrome data will be synced to the user's Google account by saving that data on Google's servers.

24. In my training and experience, evidence of who was using a Google account and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

25. The stored communications and files connected to a Google account may provide direct evidence of the offenses under investigation. I know that instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Google can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example,

because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account.

Additionally, stored electronic data may provide more precise information about the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email or saved to cloud storage). Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

26. Finally, stored electronic data frequently provides relevant insight into the account owner's state of mind as it relates to the offense under investigation. For example, information in the account may indicate the owner's motive and intent to commit a crime including communications, browser and search history relating to preparation to commit crimes, or consciousness of guilt, such as deleting communications or other inculpatory data in an effort to conceal them from law enforcement. Photographs and videos can provide visual evidence of a coconspirator's participation in a critical meeting and help to identify other participants in the conspiracy who were previously unknown to law enforcement.

27. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., browser history indicating planning or preparation to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement). Other information connected to a Google account may lead to the discovery of additional evidence. For example, the identification of apps downloaded from Google may reveal services used in furtherance of

the crimes under investigation or services used to communicate with co-conspirators. A list of apps might reveal banking institutions and online trading accounts used by the targets, or the identification of other means and methods of communication. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

28. Therefore, Google's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Google's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users and other participants in the criminal conduct under investigation.

III. CONCLUSION

29. I submit that this affidavit supports probable cause for a search warrant to be served on Google as to information associated with the accounts described in Attachment A to seek the items described in Attachment B. Upon receipt of the search warrant Google will then compile the requested records at a time convenient to it, thus reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

WHEREFORE, your deponent respectfully requests that a search warrant be issued for information associated with a certain Email Account, specifically: "mcgolfo@gmail.com" (the "SUBJECT EMAIL ACCOUNT"), that is stored at premises controlled by Google, Inc. ("Google") an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043 as further described in Attachment A, to search for and seize the items listed in Attachment B as evidence and instrumentalities of violations of 18 U.S.C. § 666 and 18 U.S.C.

§ 1347(a).

California 94043 as further described in Attachment A, to search for and seize the items listed in Attachment B as evidence and instrumentalities of violations of 18 U.S.C. § 666 and 18 U.S.C. § 1347(a).

Respectfully submitted,



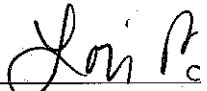
MELISSA GALICIA

Special Agent

Federal Bureau of Investigation

Subscribed and sworn to before me

on 3/27/19



THE HONORABLE
UNITED STATES
EASTERN DISTRICT

s/Bloom

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with a certain email account, specifically “Mcgolfo@gmail.com” (the “SUBJECT EMAIL ACCOUNT”), that is stored at premises controlled by Google, Inc. (“Google”) an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, including any emails, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google is required to disclose the following information to the government for each account or identifier listed in Attachment A, for the time period April 1, 2015 to October 4, 2018:

a. All records or other information regarding the identification of the Accounts and the users of the Accounts, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

b. All records or other information regarding the devices associated with, or used in connection with, the Accounts, including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"),

Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International

Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the Accounts, including stored or preserved copies of emails sent to and from the accounts (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all text and voice messages (“messages”) associated with the Accounts (including voicemails, SMS messages, and MMS messages), including stored or preserved copies of messages sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each message, the date and time at which each message was sent and received, the size and length of each message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each message;

e. All Google content associated with the Accounts, including data and content associated with: Android, Gmail, Google Calendar, Google Chrome Sync, Google Contacts, Google Docs, Google Drive, Google Hangouts, Google+, Google My Maps, Google News, Google Photo, Google Profile, Google Voice, Location History, Web & App Activity, YouTube, and any other services associated with the Accounts. The Google service data and content associated with the Accounts include, without limitation: emails, voicemails, text messages, address books, contact and buddy lists, notes, reminders, calendar entries, image files, video

files, audio files, word processing documents, spreadsheets, presentations, PDFs, bookmarks, and device settings;

f. All browsing history and search history associated with the Accounts, including: Chrome browsing history, Google Search queries and history, Google Maps queries and history, Google Translate queries and history (including original text, photographs, audio files, and web page URLs submitted for translation, and the translation provided in response to such queries), and search history associated with any third-party search application or search engine;

g. All location data associated with the Accounts, including Global Positioning System ("GPS") data, cell site/cell tower triangulation/trilateration, and precision measurement information such as timing advance or per call measurement data, and Wi-Fi location, including the GPS coordinates and the dates and times of all location recordings;

h. All device backups associated with the account;

i. All Google application data and third-party application data associated with the Accounts;

j. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including Gmail logs, Google Voice logs, Google Hangouts logs, Google Drive logs, Google Play logs (including purchases, downloads, and updates of Google and third-party apps), messaging logs (including Google Hangouts, Google Voice, Google Profile, Google+, SMS, and MMS messages), password recovery logs, sign-on logs for all Google services, logs associated with device activation and upgrades, and logs associated with web-based access of Google services (including all cookies, IP addresses, browser information, and device identifiers associated with such access);

k. All other data and records, including content, relating to the services used by the Accounts;

l. All records pertaining to communications between Google and any person regarding the Accounts, including contacts with support services and records of actions taken; and

m. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Google.

II. Information to be Seized by Law Enforcement

30. Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review all information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of (i) theft concerning programs receiving federal funds, in violation of 18 U.S.C. § 666(a)(1)(A); and (ii) health care fraud, in violation of 18 U.S.C. § 1347(a), for the SUBJECT EMAIL ACCOUNT identified on Attachment A from April 1, 2015 to October 1, 2018, including:

- (a) Communications about sending money, including bank account information, and other methods of sending and receiving money;
- (b) Information regarding contact with law enforcement, access to records maintained by law enforcement, and access to fraudulent law enforcement identification materials;
- (c) Financial records, including all bank records, checks, credit card bills, and account information related to the crimes listed in this warrant;

- (c) Financial records, including all bank records, checks, credit card bills, and account information related to the crimes listed in this warrant;
- (d) Attribution evidence showing who used or owned the account at the time the records and information described in this warrant were created, edited, or deleted, including logs, phonebooks, saved usernames and passwords, documents, browsing history, photographs, videos, audio recordings, and messages;
- (e) Attribution evidence showing who used or owned electronic communications accounts and/or telephone numbers with which the owners or users of the account were in contact at the time of such communications, including contact by means of other Internet-based messaging services, email accounts, or telephone numbers;
- (f) Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscribers;
- (g) Evidence indicating the Email account owner's state of mind as it relates to the crimes under investigation;
- (h) Evidence that may identify any additional coconspirators or aiders and abettors, including records that help reveal their whereabouts;
- (i) The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s); and
- (j) The identity of the person(s) who communicated with the account about matters relating to the crimes under investigation, including their communications and records that help reveal their whereabouts.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS
RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)**

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Instagram, and my official title is _____. I am a custodian of records for Instagram. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Instagram, and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of Instagram; and
- c. such records were made by Instagram as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature